

Measuring User Satisfaction with IS Security

Reza Vaezi

Kennesaw State University

svaezi@kennesaw.edu

Wynne Chin

University of Houston

wchin@uh.edu

Abstract

Information systems security has been the focus of much academic and non-academic research. It is an important aspect of any information system and due to increasing security incidents and threats it has become a factor affecting user satisfaction with information systems. This article introduces and validates a survey instrument that measures user satisfaction with the security attribute of the system aspect of IS.

Introduction

Security is an important attribute of information systems and has been the subject of much research in IS (Whitman and Mattord 2011). Information Systems (IS) scholars researched security from different perspectives including: organizational policies and their effects on employees' security awareness and behavior (e.g. Bulgurcu et al. 2010; Crossler et al. 2013; Johnston and Warkentin 2010; Straub Jr 1990); the effects of perceived IS security on adoption of online purchasing behavior (e.g. Chang and Chen 2009; Kim et al. 2010; Liu et al. 2008; Salisbury et al. 2001); effects of IS security breaches on organizations and employees (e.g. Berezina et al. 2012; Farahmand et al. 2003); and the effects of perceived security on user satisfaction (e.g. Berezina et al. 2012; Dinev et al. 2009; Etezadi-Amoli and Farhoomand 1996; Szymanski and Hise 2000).

Results of a national survey on security and privacy indicated that US organizations were reporting a 65% reduction in customer satisfaction due to information systems security breaches (Technologies 2008). Information system security has long been found to influence user satisfaction with IS (e.g. Etezadi-Amoli and Farhoomand 1996; Kim et al. 2010; Sharma and Li 2013; Szymanski and Hise 2000) and by extension IS security would affect outcomes of user satisfaction such as consumer loyalty and intention adopt or purchase (Salisbury et al. 2001). Many studies tried to capture users' perception of security in their attempts to measure user satisfaction and/or its outcomes (e.g. Berezina et al. 2012; Dinev et al. 2009; Etezadi-Amoli and Farhoomand 1996; Szymanski and Hise 2000). Montesdioca and Maçada (2015) measured user satisfaction with information systems security practices. They focused on information systems security policy, training and overall practices. However, to the authors' knowledge, no study has yet tried to measure user satisfaction with IS security as it relates to the technical system and mechanics of interaction.

According to attribute satisfaction theory (Bettman 1974; Fishbein 1972), consumer satisfaction with a product or service is derived from consumer satisfaction with the attributes of the product or service. For example, customers' satisfaction of a dining experience is an aggregated function of their satisfaction with food (taste, look, smell, freshness, etc.) and service (courteous, timely, friendly, etc.). Applying attribute satisfaction theory to the IS context, we can think of overall user satisfaction with IS as an aggregated function of user satisfaction with different attributes of IS, one of which being the IS security. Thus, it is important to develop valid and reliable measures to capture user satisfaction with IS security. These measures, in addition to helping researchers and practitioners to gain better understanding of overall user satisfaction, give them the power to reliably capture user satisfaction with IS security and act on the findings to improve the system security if necessary.

Literature Review

Review of the literature revealed that the majority of the IS security studies are concerned with different aspects of security such as the role of employees' involvement in IT security (Dinev et al. 2009), security

threats and incidents (Farahmand et al. 2003), and security counter measures (Straub and Welke 1998). This article specifically focuses on studies of IS security that examine the relationship between system security and user satisfaction and its antecedents (continued usage, loyalty, intention to use, etc.). The effects of perceived IS security on adoption and use of systems becomes particularly important in non-mandatory information systems that deal with general consumers. Specifically, IS security is found to be directly related to consumers' adoption of online retailers (Chang and Chen 2009). Online transactions involve transmission of sensitive consumer data such as address and credit card information. As a result, negative perception about the security of online transactions has been found a major factor adversely affecting consumers' adoption of online retail (Chang and Chen 2009; Schaupp and Bélanger 2005).

Berezina et al. (2012) exposed customers to three security related scenarios (negative, neutral, and positive) in the hotel industry and then measured customers satisfaction, referral likelihood, and revisit intentions. The researchers found that negative and neutral security breach scenarios resulted in negative outcomes, regardless of whether or not customer credit card data were compromised. They also reported that the positive scenario (which told customers that the hotel has just passed a comprehensive information systems security check) resulted in increased satisfaction and revisit intentions. Schaupp and Bélanger (2005) also provided a conceptual model which indicated that privacy and security are two important factors affecting consumer satisfaction with online services.

Kim et al. (2010) investigated the effects of perceived security on adoption of e-payment systems by consumers and stated that consumers' perceived security is positively associated with their adoption and use of e-payment systems. Chang and Chen (2009) reported that consumers' perceived security of online transactions influenced their satisfaction with the online service and as result would affect their loyalty. The report also suggested that positively assessed security increases switching cost and is a good strategy to lock the customers in. They further suggested that website interface quality affects consumers' perception of security. Liu et al. (2008) constructed and tested a model of Chinese consumer satisfaction with online retailing and reported that website security had strong and positive effects on consumer satisfaction. Moreover, Szymanski and Hise (2000) investigated the factors affecting consumer satisfaction with online retailers. They modeled transaction security and reported that security had a significant effect on consumer satisfaction with online retailers.

In an effort to investigate the relationship between user satisfaction and user performance, Etezadi-Amoli and Farhoomand (1996) developed an instrument that included system security in measuring user satisfaction and its connection with performance. Palvia (1996) developed a model, that included security and integrity to measure small business satisfaction with Information Systems. However, his security measures failed to demonstrate an acceptable level of reliability.

Goodhue and Straub (1991) defined and measured user satisfactoriness with system security. They proposed that user satisfactoriness is different from user satisfaction in that it refers to the extent to which the information system helps the user perform tasks, while user satisfaction refers to the extent to which a user's personal needs are satisfied by using the system. They developed a survey to measure user satisfactoriness. However, the instrument suffered from numerous design problems as stated by them. They also did not find adequate support for their proposed model, which they partly attributed to the poor survey instrument and study design.

Montesdioca and Maçada (2015) introduced a model of user satisfaction with information systems security practices (security policy and training) implemented by Brazilian organizations. Their model stated that user perception of information systems performance and effort-benefit ratio affects user satisfaction with information systems security practices.

It is evident from the literature that no study has attempted to directly measure user satisfaction with information systems security as it pertains to technical aspect of the system as opposed to security policies and practices implemented by organizations. To that end, this study develops and validates a set of items that can measure user satisfaction with system security directly. The outcome of this study can be incorporated in future research focusing on user satisfaction and IS security.

Item Development

The content validity of a set of questionnaire items refers to how representative the items are of the construct they intend to measure (Ives et al. 1983). Therefore, having a clear understanding of a construct is a necessary condition for developing survey items that tend to measure the construct (Straub et al. 2004). To that end, this research adopted Whitman and Mattord (2011) definition of IS security and modified it for the study context. Information systems security is defined as the extent to which the information in the system is kept safe. Related measures of system security satisfaction are therefore developed based on the adopted definition.

Review of consumer behavior literature on consumer satisfaction and IS literature on user satisfaction revealed that two types of scales are commonly used to measure individual satisfaction with different products and services (e.g. Bhattacharjee 2001; Bhattacharjee and Premkumar 2004; McKinney et al. 2002; Oliver 2010). One type is semantic differential and the other is the Likert scale which is essentially a rating method. Semantic differential scale uses a set of opposing adjectives (e.g. displeased-pleased, frustrated-contented, etc.) to capture an individual's attitude towards the phenomenon under study while Likert scale uses only one adjective or action and asks individuals to rate their attitude towards the given adjective on a spectrum of strong negativity to strong positivity (e.g. strongly dissatisfied to strongly satisfied) (Schibeci 1982). Following the prevalent usage of Likert scale in the IS domain, this study developed three items to measure user satisfaction with IS security on a seven-point Likert scale ranging from strongly dissatisfied to strongly satisfied. These items read as follows:

- Overall, how satisfied are you with the extent to which the system keeps information safe?
- Overall, how satisfied are you with the extent to which information is kept secure by the system?
- Overall, how satisfied are you with the extent to which the system protects information?

Reliability and Validity

The items were examined as part of a larger study that developed and tested a survey instrument to measure user satisfaction with a variety of IS attributes as well as overall satisfaction with the system. However, this article only introduces and discusses the items measuring user satisfaction with system security attribute and refers to the main study when necessary. The items were tested using students enrolled in a core business class at a major North American university. Students were asked to evaluate their satisfaction with different aspects and attributes of an information system that they used for registering for their classes and paying tuition fees.

A total of 556 students were enrolled in all sections of the core course and they were offered two extra credits for their participation in the study. This resulted in 450 usable responses which puts the response rate at 81%. Young college students between 18 and 24 years old comprised 90% the respondents. . Male and female respondents were 55% and 45%, respectively. The majority of users (86%) indicated that they use the system actively from a few times a day to few times a month. Further, 63% of the respondents indicated that they have been using the system for more than a year, whereas 26% have been using the system for less than six months.

The reliability of a set of measures or questionnaire items refers to the stability of measures over a range of conditions. It basically reflects the accuracy of a set of items that are measuring a construct of interest. One way to demonstrate reliability is through measuring internal consistency (Straub et al. 2004). Internal consistency of the current set of items is tested through applying Cronbach's alpha test using SPSS version 22. The calculated Cronbach's alpha score is 0.93 (well above the suggested 0.80 for basic research) which indicates an excellent reliability for the items (Cronbach 1951). The questions were randomized among twenty-one other items that measured user satisfaction with other attributes of an information system. The item randomization weakened the chance of common method bias effect in inflating the reliability score. Furthermore, correlation test indicated a strong correlation among items. The calculated correlations between items 1 and 2, items 1 and 3, and items 2 and 3 are 0.829, 0.827, and 0.816 respectively.

Construct validity refers to whether items used for measuring a specific construct (e.g. security satisfaction) fit together in way that captures the essence of the construct. The construct validity can be established through convergent and discriminant validity. Convergent validity refers to how items measuring a specific construct are strongly associated with each other, whereas discriminant validity refers to how items measuring different constructs are independent from each other (Straub et al. 2004). A factor analysis using principal components methods and varimax rotation revealed that items measuring user satisfaction with system security form their own factor and are distinguishable from other constructs presented in the analysis.

Discussion and Conclusion

In this paper we argued the importance of measuring user satisfaction with information systems security and proposed a set of questions to measure it. We developed the survey questions measuring IS security based on a widespread conceptualization of IS security that we found by carefully reviewing the literature in this area. The test of the measures was conducted as part of a bigger study that was designed to capture user satisfaction with different aspects and attributes of information systems.

The results of our analysis demonstrated an excellent reliability for the proposed items in terms of measuring the construct of the interest. The construct validity was also established through principal component analysis. Overall, the results suggest that the proposed items can reliably measure user satisfaction with IS security and can be used in future research interested in measuring user satisfaction with IS security.

We acknowledge that the use of students as primary subjects may limit the generalizability of the results. However, it does not affect reliability and validity of presented items. Future, research should attempt to test the items using a more representative population of users. Furthermore, different users may hold different sensitivity towards attributes of a system. For example, system security might be very important to user A but not as important to user B. This research did not account for the importance of system security to users. We call for future research to include measures of importance in their models.

This research assumed that security as a non-decomposable attribute of information systems. Future research should expand on this research in terms of defining possible user related dimensions of IS security as well as developing measurement items for the newly identified dimensions. Future research can also try to further establish the validity and reliability of the proposed items through retesting the questions in different contexts. Another possible avenue for future endeavors is to develop semantic differential scales for the proposed set of items in this research. The current items were only tested using a Likert scale.

REFERENCES

- Berezina, K., Cobanoglu, C., Miller, B.L., and Kwansa, F.A. 2012. "The Impact of Information Security Breach on Hotel Guest Perception of Service Quality, Satisfaction, Revisit Intentions and Word-of-Mouth," *International Journal of Contemporary Hospitality Management* (24:7), 2012, pp 991-1010.
- Bettman, J.R. 1974. "A Threshold Model of Attribute Satisfaction Decisions," *Journal of Consumer Research*, pp 30-35.
- Bhattacharjee, A. 2001. "An Empirical Analysis of the Antecedents of Electronic Commerce Service Continuance," *Decision Support Systems* (32:2), p 201.
- Bhattacharjee, A., and Premkumar, G. 2004. "Understanding Changes in Belief and Attitude toward Information Technology Usage: A Theoretical Model and Longitudinal Test," *MIS Quarterly* (28:2), pp 229-254.
- Bulgurcu, B., Cavusoglu, H., and Benbasat, I. 2010. "Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness," *MIS quarterly* (34:3), pp 523-548.
- Chang, H.H., and Chen, S.W. 2009. "Consumer Perception of Interface Quality, Security, and Loyalty in Electronic Commerce," *Information & Management* (46:7), pp 411-417.
- Cronbach, L.J. 1951. "Coefficient Alpha and the Internal Structure of Tests," *psychometrika* (16:3), pp 297-334.
- Crossler, R.E., Johnston, A.C., Lowry, P.B., Hu, Q., Warkentin, M., and Baskerville, R. 2013. "Future Directions for Behavioral Information Security Research," *Computers & Security* (32:0), 2//, pp 90-101.
- Dinev, T., Goo, J., Hu, Q., and Nam, K. 2009. "User Behaviour Towards Protective Information Technologies: The Role of National Cultural Differences," *Information Systems Journal* (19:4), pp 391-412.

- Etezadi-Amoli, J., and Farhoomand, A.F. 1996. "A Structural Model of End User Computing Satisfaction and User Performance," *Information & Management* (30:2), pp 65-73.
- Farahmand, F., Navathe, S.B., Enslow, P.H., and Sharp, G.P. 2003. "Managing Vulnerabilities of Information Systems to Security Incidents," *Proceedings of the 5th international conference on Electronic commerce*: ACM, pp. 348-354.
- Fishbein, M. 1972. *The Search for Attitudinal-Behavioral Consistency*. New York: The Free Press.
- Goodhue, D.L., and Straub, D.W. 1991. "Security Concerns of System Users: A Study of Perceptions of the Adequacy of Security," *Information & Management* (20:1), 1//, pp 13-27.
- Ives, B., Olson, M.H., and Baroudi, J.J. 1983. "The Measurement of User Information Satisfaction," *Communications of the ACM* (26:10), pp 785-793.
- Johnston, A.C., and Warkentin, M. 2010. "Fear Appeals and Information Security Behaviors: An Empirical Study," *MIS quarterly* (34:3), pp 549-566.
- Kim, C., Tao, W., Shin, N., and Kim, K.-S. 2010. "An Empirical Study of Customers' Perceptions of Security and Trust in E-Payment Systems," *Electronic Commerce Research and Applications* (9:1), 1//, pp 84-95.
- Liu, X., He, M., Gao, F., and Xie, P. 2008. "An Empirical Study of Online Shopping Customer Satisfaction in China: A Holistic Perspective," *International Journal of Retail & Distribution Management* (36:11), pp 919-940.
- McKinney, V., Kanghyun, Y., and Zahedi, F.M. 2002. "The Measurement of Web-Customer Satisfaction: An Expectation and Disconfirmation Approach," *Information Systems Research* (13:3), pp 296-315.
- Montesdioca, G.P.Z., and Maçada, A.C.G. 2015. "Measuring User Satisfaction with Information Security Practices," *Computers & Security* (48:0), 2//, pp 267-280.
- Oliver, R.L. 2010. *Satisfaction: A Behavioral Perspective on the Consumer*. Armonk: NY: M.E. Sharpe.
- Palvia, P.C. 1996. "A Model and Instrument for Measuring Small Business User Satisfaction with Information Technology," *Information & Management* (31:3), pp 151-163.
- Salisbury, W.D., Pearson, R.A., Pearson, A.W., and Miller, D.W. 2001. "Perceived Security and World Wide Web Purchase Intention," *Industrial Management & Data Systems* (101:4), pp 165-177.
- Schaupp, L.C., and Bélanger, F. 2005. "A Conjoint Analysis of Online Consumer Satisfaction," *Journal of Electronic Commerce Research* (6:2), pp 95-111.
- Schibeci, R. 1982. "Measuring Student Attitudes: Semantic Differential or Likert Instruments?," *Science Education* (66:4), pp 565-570.
- Sharma, G., and Li, B. 2013. "Customer Satisfaction in Web 2.0 and Information Technology Development," *Information Technology & People* (26:4), 2013, pp 347-367.
- Straub, D., Boudreau, M.-C., and Gefen, D. 2004. "Validation Guidelines for Is Positivist Research," *The Communications of the Association for Information Systems* (13:1), p 63.
- Straub, D.W., and Welke, R.J. 1998. "Coping with Systems Risk: Security Planning Models for Management Decision Making," *MIS Quarterly* (22:4), pp 441-469.
- Straub Jr, D.W. 1990. "Effective Is Security: An Empirical Study," *Information Systems Research* (1:3), pp 255-276.
- Szymanski, D.M., and Hise, R.T. 2000. "E-Satisfaction: An Initial Examination," *Journal of retailing* (76:3), pp 309-322.
- Technologies, C. 2008. "As Security Threats Proliferate, U.S. Organizations Report More Incidents of Confidential Information Loss and Decreasing Levels of Customer Satisfaction," in: *Business Wire*. New York.
- Whitman, M.E., and Mattord, H.J. 2011. *Principles of Information Security*. Course Technology Ptr.